

**Attack,  
Defense,  
& Analysis of  
Vulnerable  
Networks**

# **Final Engagement**

## **Team 2**





# Table of Contents

**01** Network Topology

**02** Alerts Implemented

**03** Hardening

**04** Implementing Patches



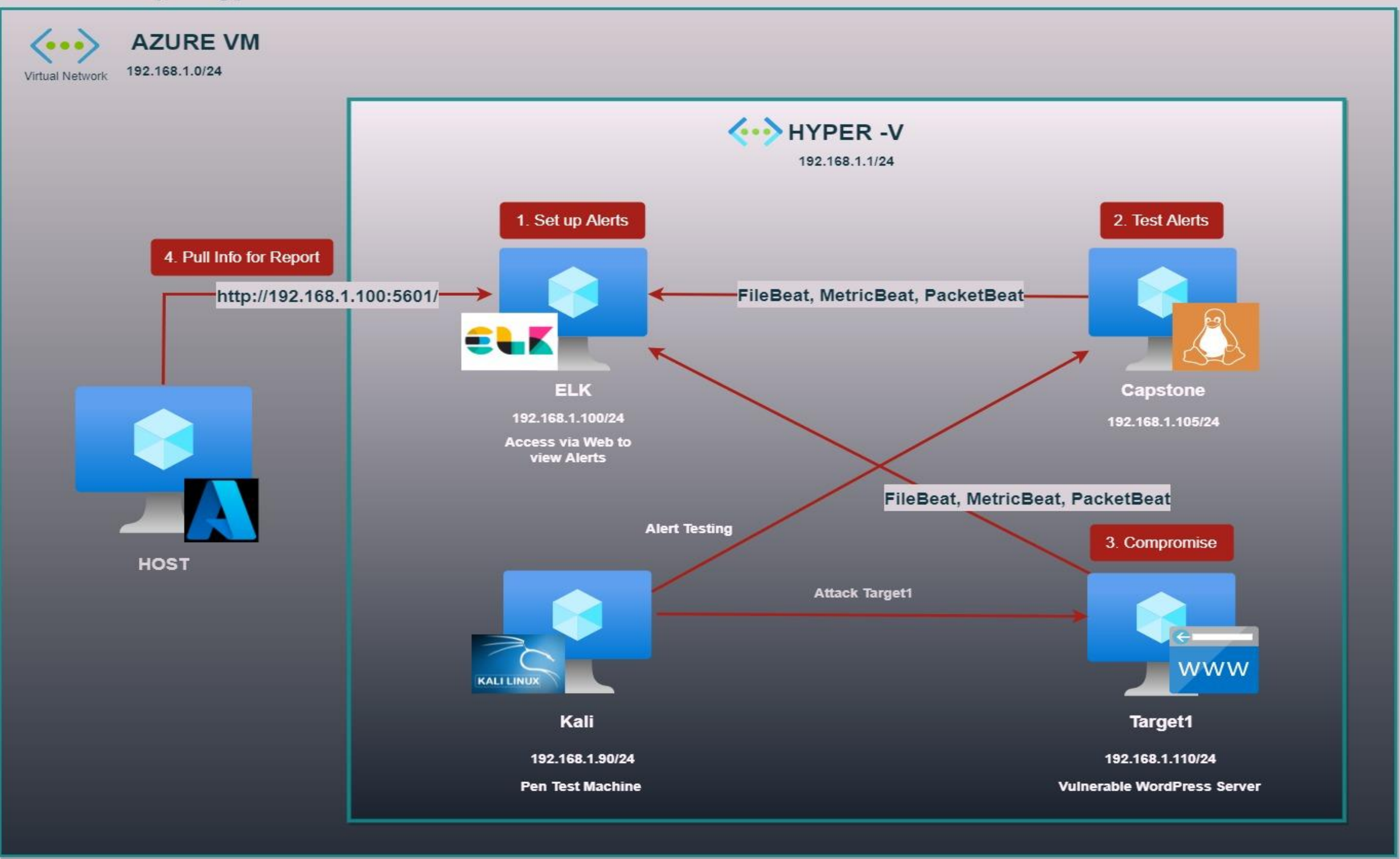
A network topology diagram is overlaid on a background of server racks. The diagram features a central cloud icon connected to six other nodes: a smartphone, a laptop, a server rack, a database cylinder, a camera, and a desktop monitor. These nodes are further interconnected with each other, forming a mesh-like structure. The background shows rows of server racks with blue indicator lights.

# **Network Topology & Critical Vulnerabilities**



# Network Topology

## Network Topology



### Network

Address Range:192.168.1.0/24  
Netmask: 255.255.255.0  
Gateway: 192.168.1.1

### Machines

IPv4:192.168.1.1  
OS: Windows 10  
Hostname: HyperV host

IPv4: 192.168.1.100  
OS: Linux  
Hostname:ELK

IPv4: 192.168.1.105  
OS: Linux  
Hostname:Capstone

IPv4:192.168.1.110  
OS:Linux  
Hostname: Target 1

IPv4: 192.168.1.90  
OS: Linux  
Hostname:Kali

# Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
<b>CVE-2014-5266</b> Wordpress XMLRPC DoS	Wordpress XMLRPC is vulnerable to a XML based denial of service. This vulnerability affects WordPress 3.5 - 3.92.2 (3.8.4 and 3.7.4 are also patched)	<b>Medium Impact (CVSS Score: 5.0)</b> The Incutio XML-RPC (IXR) Library, as used in WordPress before 3.9.2 and Drupal 6.x before 6.33 and 7.x before 7.31, does not limit the number of elements in an XML document, which allows remote attackers to cause a denial of service (CPU consumption) via a large document
<b>CVE-2013-0235</b> Wordpress Pingback Locator	The XMLRPC API in WordPress before 3.5.1 This module will scan for WordPress sites with the Pingback API enabled. By interfacing with the API an attacker can cause the WordPress site to port scan an external target and return results.	<b>Medium Impact (CVSS Score: 6.4)</b> Allows remote attackers to send HTTP requests to intranet servers, and conduct port-scanning attacks, by specifying a crafted source URL for a pingback, related to a Server-Side Request Forgery (SSRF) issue.
<b>CVE-2015-0235</b> Wordpress XMLRPC GHOST Vulnerability Scanner. (It is called the GHOST vulnerability as it can be triggered by the GetHOST functions)	Remote code execution vulnerability impacting older versions of the GNU C Library (glibc versions less than 2.18). This is an implementation problem in the affected versions of the Linux software.	<b>Critical Impact (CVSS Score: 10.0)</b> A remote attacker is able to make an application call to the gethostbyname or gethostbyname2 functions, and use this flaw to execute arbitrary code with the permissions of the user running the application.





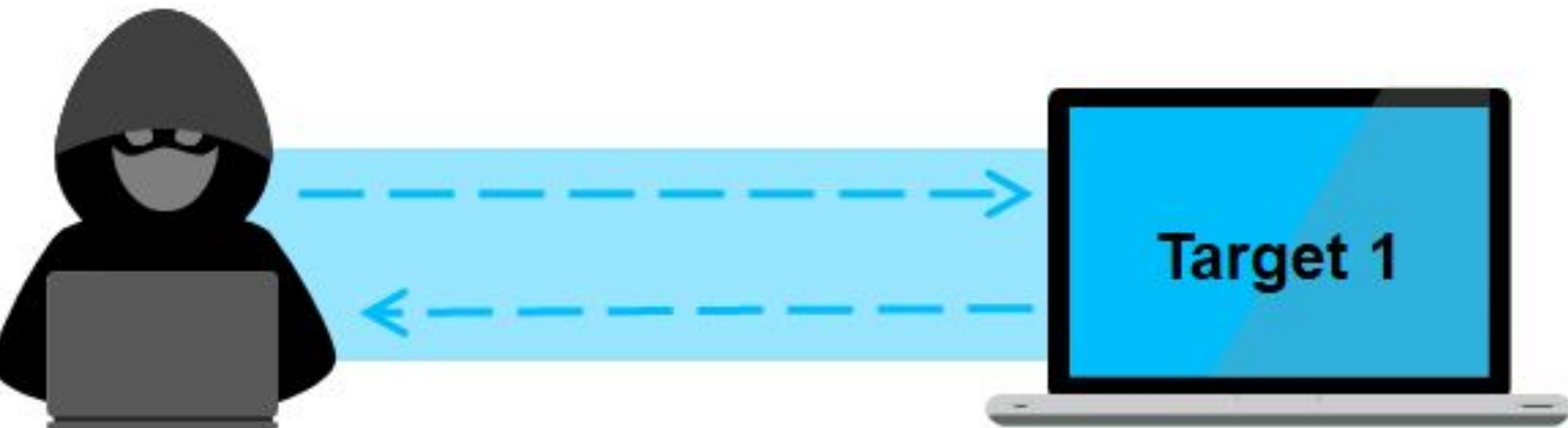
# Alerts Implemented

# Excessive HTTP Errors

Alert 1 is implemented as follows:

WHEN count() GROUPED OVER top 5  
'http.response.status\_code' IS ABOVE 400 FOR THE  
LAST 5 minutes

- Metric: HTTP Errors
- Threshold: Above 400 for the last 5 minutes
- Vulnerability Mitigated: Brute Force Attacks. Resource Usage Issues.



Current status for 'Excessive HTTP Errors' [Deactivate](#) [Delete](#)

Execution history

Action statuses

Last one hour ▾

Trigger time	State	Comment
2022-02-12T01:19:21+00:00	✓ OK	
2022-02-12T01:18:21+00:00	✓ OK	
2022-02-12T01:17:21+00:00	✓ OK	
2022-02-12T01:16:21+00:00	✓ OK	
2022-02-12T01:15:21+00:00	✓ OK	
2022-02-12T01:14:21+00:00	✓ OK	
2022-02-12T01:13:21+00:00	✓ OK	
2022-02-12T01:12:21+00:00	✓ OK	
2022-02-12T01:11:21+00:00	✓ OK	
2022-02-12T01:10:21+00:00	✓ OK	

Rows per page: 10 ▾

< 1 ... 14 15 16 17 18 ... 23 >



# HTTP Request Size Monitor

Alert 2 is implemented as follows:

WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute

- Metric: http.request.bytes
- Threshold: Above 3500 for the last minute
- Vulnerability Mitigated: DoS (Denial of Service) Attacks.

Current status for 'http request size monitor' Deactivate Delete

Execution history

Action statuses

Last 7 days

Trigger time	State	Comment
2022-02-12T00:13:37+00:00	✓ OK	
2022-02-12T00:12:37+00:00	✓ OK	
2022-02-12T00:11:37+00:00	▷ Firing	
2022-02-12T00:10:36+00:00	▷ Firing	
2022-02-12T00:09:36+00:00	▷ Firing	
2022-02-12T00:08:36+00:00	▷ Firing	
2022-02-12T00:07:36+00:00	▷ Firing	
2022-02-12T00:06:36+00:00	▷ Firing	
2022-02-12T00:05:36+00:00	✓ OK	
2022-02-12T00:04:36+00:00	✓ OK	

Rows per page: 10

<

1

...

20

21

22

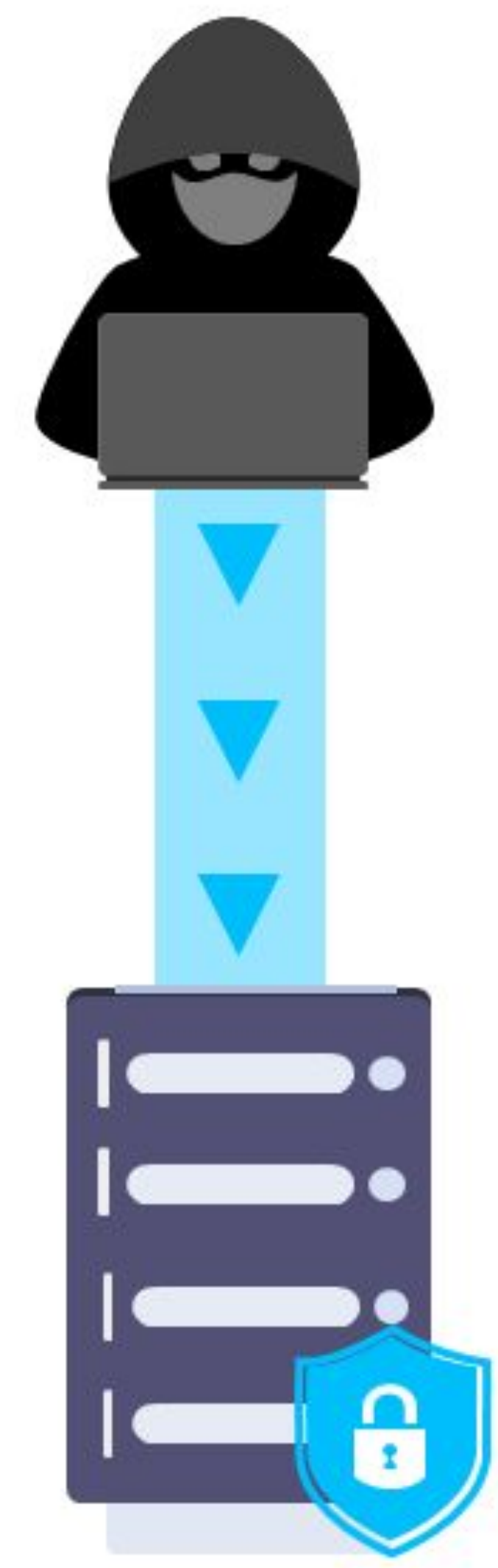
23

24

...

26

>





# CPU Usage Monitor

Alert 3 is implemented as follows:

WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

- Metric: system.process.cpu.total.pct
- Threshold: Above 0.5 for the last 5 minutes.
- Vulnerability Mitigated: Resource Management, Excessive CPU Usage.

Current status for 'cpu usage monitor' Deactivate Delete

Execution history

Action statuses

Last 7 days

Trigger time	State	Comment
2022-02-13T10:04:50+00:00	✓ OK	
2022-02-13T10:03:49+00:00	✓ OK	
2022-02-13T10:02:49+00:00	✓ OK	
2022-02-13T10:01:50+00:00	▷ Firing	
2022-02-13T10:00:50+00:00	▷ Firing	
2022-02-13T09:59:50+00:00	▷ Firing	
2022-02-13T09:58:50+00:00	▷ Firing	
2022-02-13T09:57:50+00:00	▷ Firing	
2022-02-13T09:56:49+00:00	▷ Firing	
2022-02-12T03:29:37+00:00	✓ OK	

Rows per page: 10

<

1

...

40

41

42

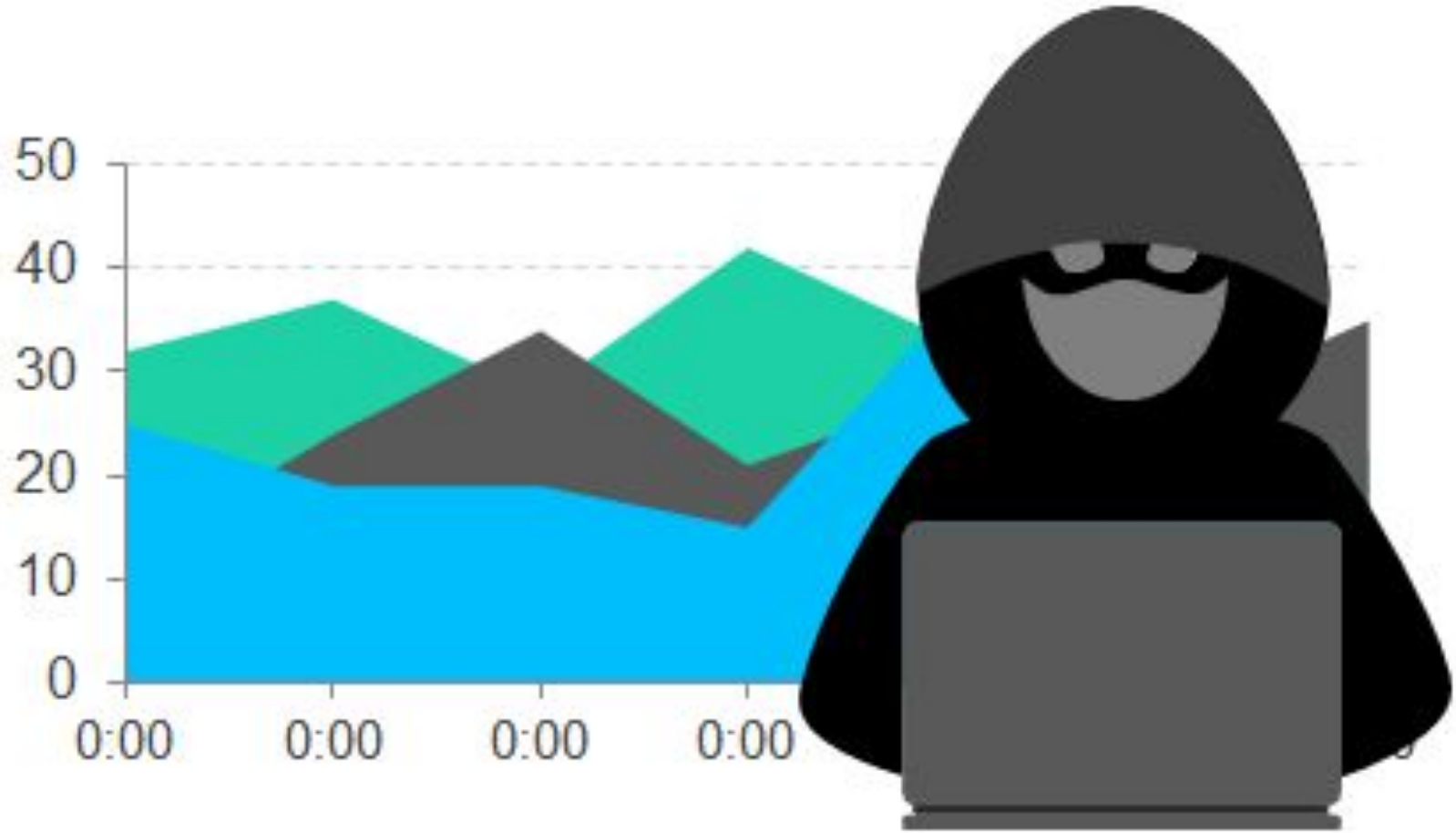
43

44

...

62

>







# Hardening

Reducing System Vulnerabilities



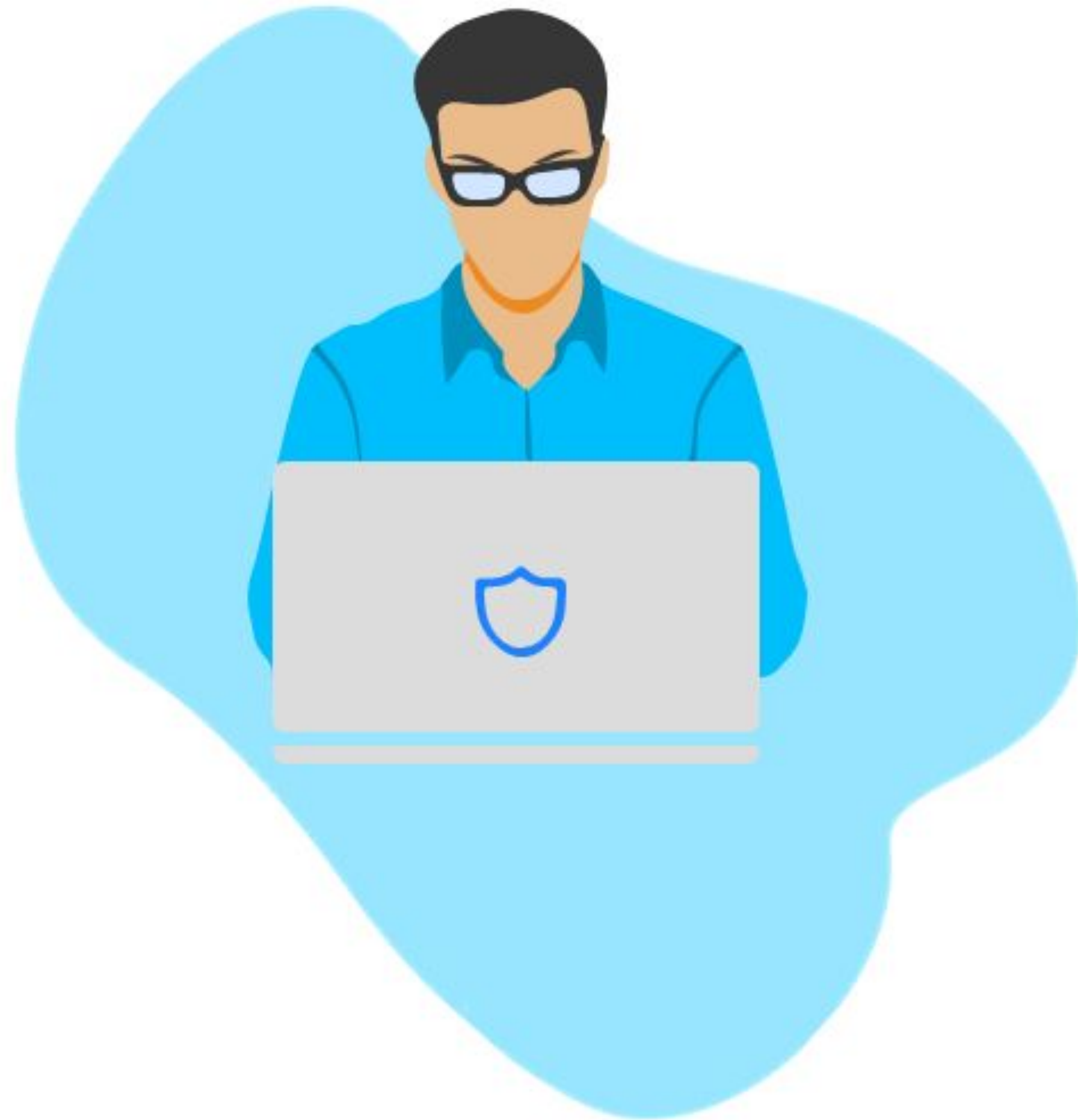
# Hardening Against CVE-2014-5266

- Update current version of WordPress (4.8.7) to the latest release.
- Completing this update prevents:
  - Information disclosure via XML entity attacks,
  - Fixes a possible code execution when processing widgets,
  - And adds protections against brute force attacks against CSRF Tokens.
- This update can either be installed individually on the server by performing an OS distribution update, or by downloading the latest software the WordPress vendor.





# Hardening Against CVE-2013-0235



- Update current version of Wordpress (4.8.7) to the latest release.
- Completing this update stops an attacker from triggering a buffer overflow when an invalid hostname argument is supplied.



# Hardening Against CVE-2015-0235

- Update to the latest version of Debian Linux (8.11). It is recommended upgrading away from version 8 as this version is end of life since 2020.
- Upgrading will prevent this arbitrary remote code execution vulnerability as it has been addressed in the latest releases.
- Carrying out this update can be completed by executing a distribution update: `sudo apt-get update` directly on a server. Alternatively, this can also be deployed to several servers using ansible.





# Security

## IMPLEMENTING PATCHES

```
- name: restart system to reboot to newest kernel  
  shell: "sleep 5 && reboot;  
  async: 1  
  poll: 0  
- name: wait for 10 seconds  
  pause:  
    seconds: 10  
- name: wait for the system to reboot  
  wait_for_connection:  
    connect_timeout: 20  
    sleep: 5  
    delay: 5  
    timeout: 60
```





# Implementing Patches with Ansible

## Playbook Overview

This Playbook addresses the first two vulnerabilities by updating WordPress to the latest version.

YAML

# Updating WordPress

- name: Update WordPress

  - unarchive:

    - src: <https://wordpress.org/latest.tar.gz>

    - dest: "/var/www"

    - remote\_src: yes

    - creates: "/var/www/wordpress"

# Setup permissions

- name: permissions for directories

  - shell: "/usr/bin/find /var/www/wordpress/ -type d -exec chmod 750 {} \;"

- name: permissions for files

  - shell: "/usr/bin/find /var/www/wordpress/ -type f -exec chmod 640 {} \;"






# Implementing Patches with Ansible

## Playbook Overview

This Playbook addresses the first two vulnerabilities by updating authentication for MySQL database.



```
# MySQL Configuration
- name: Set the root password
  mysql_user:
    name: root
    password: "{{ mysql_root_password }}"
    login_unix_socket: /var/run/mysqld/mysqld.sock
- name: Remove all anonymous user accounts
  mysql_user:
    name: ""
  host_all: yes
  state: absent
  login_user: root
  login_password: "{{ mysql_root_password }}"
```




# Implementing Patches with Ansible

## Playbook Overview

This Playbook addresses the third vulnerabilities by updating the Linux distribution to the latest version.

This may also address the WordPress vulnerabilities, as available patches in the repository would also get installed.

For zero-day vulnerabilities, it is advisable to download SW specific patches directly from the software vendor.



```
YAML
# Updating OS distribution
---
- hosts: servers
  become: true
  become_user: root
  tasks:
    - name: Update apt repo and cache on all Debian/Ubuntu boxes
      apt: update_cache=yes force_apt_get=yes cache_valid_time=3600
    - name: Upgrade all packages on servers
      apt: upgrade=dist force_apt_get=yes
```